1

1 / 1 point

The primary limitation of 3DES is its slow operation in software.

Correct answer:

True

False

**Results for question 2.**

2

1 / 1 point

A device that uses a seemingly random source, often labeled an entropy source, as its input is a \_\_\_\_\_\_\_\_.



PSRN

, Not Selected



PRF

, Not Selected



PRNG

, Not Selected

Correct answer:



TRNG

**Results for question 3.**

3

1 / 1 point

The algorithm responsible for various changes and conversions on the plaintext is the \_\_\_\_\_\_\_\_\_.

Correct answer:



encryption



keystream

, Not Selected



cipher

, Not Selected



codebook

, Not Selected

**Results for question 4.**

4

1 / 1 point

The security of a symmetric block cipher intensifies with the addition of more rounds.

Correct answer:

True

False

**Results for question 5.**

5

0 / 1 point

The composition of a symmetric encryption scheme includes \_\_\_\_\_\_\_\_\_ essential components.

Incorrect answer:



three

Correct Answer:

five



four

, Not Selected



five

, Not Selected



six

, Not Selected

**Results for question 6.**

6

1 / 1 point

The foundational structure seen in many symmetric block encryption algorithms like DES was initially outlined by \_\_\_\_\_\_\_\_\_ at IBM in 1973.

Correct answer:

Horst Feistel

**Results for question 7.**

7

1 / 1 point

\_\_\_\_\_\_\_\_\_, a stream cipher, is integral to the Secure Sockets Layer/Transport Layer Security standards for browser-server communication and is a component of WEP and WPA protocols.

Correct answer:

RC4

**Results for question 8.**

8

0 / 1 point

An encryption method is considered \_\_\_\_\_\_\_\_\_ when the resources needed to decipher it surpass the value of the information or when the deciphering time outlasts the information's relevance.

Incorrect answer:

secure

Correct Answer:computationally secure

**Results for question 9.**

9

1 / 1 point

Conventional encryption, secret-key, or single-key encryption is synonymous with public-key encryption.

True

Correct answer:

False

**Results for question 10.**

10

0 / 1 point

Before the advent of public-key encryption in the late 1970s, the encryption method universally employed, synonymous with conventional, secret-key, or single-key encryption, was \_\_\_\_\_\_\_\_\_.

Incorrect answer:

symmetric key encryption

Correct Answer:symmetric

1

1 / 1 point

In terms of speed and code size, stream ciphers generally outpace block ciphers.

Correct answer:

True

False

### Results for question 2.

2

1 / 1 point

Encryption algorithms fundamentally lean on two principles: \_\_\_\_\_\_\_\_\_, where each plaintext element is substituted with another, and transposition, which rearranges the plaintext elements.

Correct answer:

substitution

### Results for question 3.

3

1 / 1 point

The security of a symmetric block cipher intensifies with the addition of more rounds.

Correct answer:

True

False

### Results for question 4.

4

1 / 1 point

When the analyst persuades the system to input a specifically crafted message, it opens up the system to a \_\_\_\_\_\_\_\_\_ attack.



known plaintext

, Not Selected

Correct answer:



chosen plaintext



ciphertext only

, Not Selected



chosen ciphertext

, Not Selected

### Results for question 5.

5

1 / 1 point

\_\_\_\_\_\_\_\_\_, a stream cipher, is integral to the Secure Sockets Layer/Transport Layer Security standards for browser-server communication and is a component of WEP and WPA protocols.

Correct answer:

RC4

### Results for question 6.

6

1 / 1 point

The foundational structure seen in many symmetric block encryption algorithms like DES was initially outlined by \_\_\_\_\_\_\_\_\_ at IBM in 1973.

Correct answer:

Horst Feistel

### Results for question 7.

7

0 / 1 point

Three chief cryptographic methods utilized for PRNGs include: Asymmetric ciphers, Hash functions and message authentication codes, and \_\_\_\_\_\_\_\_\_.

Incorrect answer:

Symmetric ciphers

Correct Answer:symmetric block ciphers

### Results for question 8.

8

1 / 1 point

The \_\_\_\_\_\_\_\_\_ mode can operate solely with the encryption function, bypassing the need for decryption.



DKS

, Not Selected



CBC

, Not Selected



ECB

, Not Selected

Correct answer:



CTR

### Results for question 9.

9

1 / 1 point

In the \_\_\_\_\_\_\_\_ mode, a flaw in a block of transmitted ciphertext affects only its corresponding plaintext block.



CBC

, Not Selected



TSR

, Not Selected

Correct answer:



ECB



CTS

, Not Selected

### Results for question 10.

10

1 / 1 point

A characteristic of a good stream cipher is that the ciphertext should exceed the plaintext in length.

True

Correct answer:

False